



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,532	07/14/2001	Antony John Rogers	063170.6291	3485
5073	7590	03/11/2010		
BAKER BOTTS L.L.P. 2001 ROSS AVENUE SUITE 600 DALLAS, TX 75201-2980			EXAMINER PYZOCHA, MICHAEL J	
			ART UNIT 2437	PAPER NUMBER
			NOTIFICATION DATE 03/11/2010	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ptomail1@bakerbotts.com
glenda.orrantia@bakerbotts.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/905,532
Filing Date: July 14, 2001
Appellant(s): ROGERS ET AL.

Todd A. Cason
(Reg. No. 54,020)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/04/2009 appealing from the Final Office action mailed 02/10/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

U.S. 6,192,512	CHESS	2-2001
U.S. 6,851,057	NACHENBERG	2-2005

U.S. 5,398,196

CHAMBERS

3-1995

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1, 4, 8-16, 20, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chess (US 6192512) in view of Nachenberg (US 6851057).

As per claims 1, 10-12, and 14, Chess discloses a method and systems of detecting viral code in subject files, comprising: creating an artificial memory region spanning one or more components of the operating system (see Fig. 2 column 4 lines 49-51); emulating execution of at least a portion of computer executable code in a subject file (see column 4 lines 33-49); monitoring attempts by the emulated computer executable code to access the artificial memory region; in response to detecting an attempt to access the artificial memory region, determining a source program that is associated with the attempt to access the artificial memory region and determining based on the attempt to access the artificial memory region that the emulated computer executable code is viral (see column 4 lines 49-54).

Chess fails to explicitly disclose the artificial memory region is associated with an export table of a dynamically-linked library; determining an export table entry of the dynamically-linked library that is associated with the attempt to access information and basing a virus determination on this entry.

However, Nachenberg teaches an export table of a dynamically-linked library as an entry point for viruses (see column 5 lines 44-67 and column 6 lines 53-64); and

monitoring these entry points (i.e. modified entries of the export table) to determine whether a virus is present (see column 8 lines 6-22 and column 9 lines 47-65).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to monitor export tables of dynamically-linked libraries in the Chess system.

Motivation to do so would have been that the export tables are a known entry point of viruses (see Nachenberg column 6 lines 53-64).

As per claims 4 and 16, the modified Chess and Nachenberg system discloses emulating functionality of the identified operating system call while monitoring the operating system call to determine whether the computer executable code is viral (see Chess column 4 lines 33-54).

As per claims 8, 9, 20 and 23, the modified Chess and Nachenberg system discloses monitoring access by the emulated computer executable code to dynamically linked functions to determine viral activity (see Nachenberg column 5 lines 44-67; column 6 lines 53-64; column 8 lines 6-22 and column 9 lines 47-65).

As per claims 13 and 15, the modified Chess and Nachenberg system discloses a fourth segment comprising auxiliary code, wherein the auxiliary code determines an operating system call that the emulated computer executable code attempted to access; a fifth segment comprising analyzer code, wherein the analyzer code monitors the operating system call to determine whether the computer executable code is viral, while emulation continues (see Chess column 4 lines 33-54).

As per claim 22, the modified Chess and Nachenberg system discloses creating an artificial memory region comprises creating a custom version of an export table with predetermined values for the entry points (see Nachenberg column 5 lines 44-67; column 6 lines 53-64; column 8 lines 6-22 and column 9 lines 47-65).

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Chess and Nachenberg system as applied to claim 1 above, and further in view of Chambers (US 5398196).

As per claim 21, the modified Chess and Nachenberg system fails to disclose monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping; and determining based on the detection of looping that the emulated computer executable code is viral.

However, Chambers teaches detecting looping to indicate a virus (see Chambers column 10 lines 40-58).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to monitor for looping in the modified Chess and Nachenberg system.

Motivation to do so would have been to prevent viruses from replicating themselves (see Chambers column 10 lines 40-58).

(10) Response to Argument

Rejection of claims 1, 4, 8-16, 20, 22 and 23 under 35 USC 103(c) over Chess in view of Nachenberg

A. Appellant argues Chess in view of Nachenberg fails to disclaim various claim limitations

1. Appellant argues the Chess-Nachenberg combination fails to disclose "in response to detecting an attempt to access the artificial memory region, determining an export table entry in the export table of the dynamically-linked library that is associated with the attempt to access the artificial memory region"

Specifically Appellant argues (see pages 16-15) that the Examiner has paraphrased the claim limitations in the rejection and therefore fails to address the actual claimed language. With respect to this argument, the Examiner has paraphrased the claim limitations to show what each reference specifically taught in relating to the claimed invention. In this section Appellant is arguing the references separately; one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Furthermore, as will be shown in the response, to Appellant's additional arguments, below the combination teaches all of the claimed limitations.

Appellant argues (see page 16) that Nachenberg does not teach an "export table entry in the export table". With respect to this argument, Appellant is directed to column 5 lines 51-52 of Nachenberg which states, "Each exported function listed in the export table 122 is an entry point into the file 100." These functions that are listed correspond to the claims "export table entry". Furthermore, in column 9 lines 49-65 and column 10 lines 3-5 Nachenberg teaches emulating code at entry points (i.e. export table entries)

to the file and reporting when a virus is found during this emulation starting at the entry point.

Appellant argues (see pages 16-17) that Nachenberg does not report which entry point is infected. Appellant further cites a portion of column 3 (incorrectly listed as column 4) as being the cited portion of the rejection. However, the Examiner did not rely on this portion of the Nachenberg reference to reject this claim limitation; column 8 lines 6-22 and column 9 lines 47-65 were relied upon to teach this limitation. In these sections at least one entry point (i.e. export table entry) is provided to determine if the file is viral and it is reported when the file is viral based on this entry point.

Appellant argues (see page 17), that Chess does not disclose determining a source program that is associated with the attempt because there is not multiple source programs between which the system determines. With respect to this argument, the claims do not require that there are multiple programs or entries in the export table to be determined between; while the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In Chess column 4 lines 49-54 it is determined that a source program is unexpectedly accessing virtual memory and is reported to an external program. In order for the reporting to occur the system must determine which one of the "new" or "suspected" files has been emulated to accurately report to the external program that the file is potentially viral. Therefore, Chess discloses determining a source program that is associated with the attempt. Furthermore, when combined with Nachenberg, this source program being tested has a

specific entry point or points (i.e. export table entry) being tested and which entry point that was tested must also be determined in order to accurately report that a file at an entry point is potentially viral. Therefore, the combination of Chess and Nachenberg teaches "in response to detecting an attempt to access the artificial memory region, determining an export table entry in the export table of the dynamically-linked library that is associated with the attempt to access the artificial memory region".

2. Appellant argues the Chess-Nachenberg combination fails to disclose "determining based on the export table entry associated with the attempt to access the artificial memory region that the emulated computer executable code is viral"

Appellant argues (see pages 18-19) that Chess does not teach determining whether a file is viral based on the export table associated with the attempt to access and Nachenberg teaches detecting viruses based on certain characteristics, but not based on the export table entry. With respect to this argument, Appellant is arguing the references separately; one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In the rejection of this claim limitation Chess was relied upon for teaching a system that determines whether emulated code is viral based on the attempted access of artificial memory (see column 4 lines 49-54). Nachenberg was relied upon for determining whether a file is viral starting at an entry point to the file. Since column 5 lines 51-52 of Nachenberg which states, "Each exported function listed

in the export table 122 is an entry point into the file 100." These entry points that are listed correspond to the claims "export table entry". Furthermore, since the entry point (i.e. export table entry) is where the virus determination starts this virus determination is based on the entry point (i.e. export table entry). When combined, the Chess-Nachenberg combination determines whether emulated code that was emulated from an entry point is viral based on the attempted access of artificial memory. Therefore, the Chess-Nachenberg combination teaches "determining based on the export table entry associated with the attempt to access the artificial memory region that the emulated computer executable code is viral".

Rejection of claim 21 under 35 USC 103(c) over Chess in view of Nachenberg and further in view of Chambers

A. Appellant argues this claim is allowable for the same reasons as above because it depends from claim 1

This argument is moot in view of the response above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Michael Pyzocha/

Primary Examiner, Art Unit 2437

Conferees:

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437